PATENT COOPERATION TREATY

From the INTERNATIONAL BUREAU

PCT

NOTIFICATION OF ELECTION

(PCT Rule 61.2)

To:

Commissioner
US Department of Commerce
United States Patent and Trademark Office, PCT
2011 South Clark Place Room CP2/5C24
Arlington, VA 22202
ETATS-UNIS D'AMERIQUE

in its capacity as elected Office

Date of mailing (day/month/year) 05 February 2001 (05.02.01)	
International application No. PCT/US00/06110	**Applicant's or agent's file reference** STS131PCT
International filing date (day/month/year) 10 March 2000 (10.03.00)	**Priority date** (day/month/year) 11 March 1999 (11.03.99)
Applicant SCHEIDT, Edward, M.	

1. The designated Office is hereby notified of its election made:

[X] in the demand filed with the International Preliminary Examining Authority on:

10 October 2000 (10.10.00)

[ ] in a notice effecting later election filed with the International Bureau on:

2. The election [X] was

[ ] was not

made before the expiration of 19 months from the priority date or, where Rule 32 applies, within the time limit under Rule 32.2(b).

The International Bureau of WIPO **34, chemin des Colombettes** **1211 Geneva 20, Switzerland**	Authorized officer Claudio Borton
Facsimile No.: (41-22) 740.14.35	Telephone No.: (41-22) 338.83.38

PATENT COOPERATION TREATY 09/936315

From the
INTERNATIONAL PRELIMINARY EXAMINING AUTHORITY

To:
Thomas M. Champagne
Rabin & Champagne, P.C.
1101 14th Street, N.W.
Suite 500
Washington, DC 20005

PCT

NOTIFICATION OF TRANSMITTAL OF INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Rule 71.1)

Date of Mailing *(day/month/year)*	20 AUG 2001
Applicant's or agent's file reference STS131PCT	**IMPORTANT NOTIFICATION**

International application No.	International filing date *(day/month/year)*	Priority date *(day/month/year)*
PCT/US00/06110	10 March 2000 (10.03.2000)	11 March 1999 (11.03.1999)

Applicant

TECSEC, INCORPORATED

1. The applicant is hereby notified that this International Preliminary Examining Authority transmits herewith the international preliminary examination report and its annexes, if any, established on the international application.

2. A copy of the report and its annexes, if any, is being transmitted to the International Bureau for communication to all the elected Offices.

3. Where required by any of the elected Offices, the International Bureau will prepare an English translation of the report (but not of any annexes) and will transmit such translation to those Offices.

4. **REMINDER**

The applicant must enter the national ase before each elected Office by performing certain acts (filing translations and paying national fees) thin 30 months from the priority date (or later in some Offices)(Article 39(1))(see also the reminder sent by t International Bureau with Form PCT/IB/301).

Where a translation of the internation application must be furnished to an elected Office, that translation must contain a translation of any annexes to he international preliminary examination report. It is the applicant's responsibility to prepare and furnish su h translation directly to each elected Office concerned.

For further details on the applicable t e limits and requirements of the elected Offices, see Volume II of the PCT Applicant's Guide.

Name and mailing address of the IPEA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer Gail O. Hay James R. Matthews Telephone No. (703) 305-9711

Form PCT/IPEA/416 (July 1992)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference STS131PCT	**FOR FURTHER ACTION**	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/US00/06110	International filing date *(day/month/year)* 10 March 2000 (10.03.2000)	Priority date *(day/month/year)* 11 March 1999 (11.03.1999)
International Patent Classification (IPC) or national classification and IPC IPC(7): G 06 F 12/14; G 06 F 17/21; G06 F 17/60 and US Cl.: 713/189; 705/2, 51; 707/500		
Applicant TECSEC, INCORPORATED		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 7 sheets, including this cover sheet.

   ☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 0 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of report with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
   - VI ☐ Certain documents cited
   - VII ☒ Certain defects in the international application
   - VIII ☐ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
10 October 2000 (10.10.2000)	16 July 2001 (16.07.2001)
Name and mailing address of the IPEA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer Gail O. Hayes Telephone No. (703) 305-9711

Form PCT/IPEA/409 (cover sheet)(July 1998)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International Application No.
PCT/US00/[redacted]110

I. Basis of the report

1. With regard to the **elements** of the international application:*

☒ the international application as originally filed.

☒ the description:
pages 1-19 as originally filed
pages NONE , filed with the demand
pages NONE , filed with the letter of _____.

☒ the claims:
pages 20-23 , as originally filed
pages NONE , as amended (together with any statement) under Article 19
pages NONE , filed with the demand
pages NONE , filed with the letter of _____.

☒ the drawings:
pages 1-3 , as originally filed
pages NONE , filed with the demand
pages NONE , filed with the letter of _____.

☐ the sequence listing part of the description:
pages NONE , as originally filed
pages NONE , filed with the demand
pages NONE , filed with the letter of _____.

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language _____ which is:

☐ the language of a translation furnished for the purposes of international search (under Rule23.1(b)).

☐ the language of publication of the international application (under Rule 48.3(b)).

☐ the language of the translation furnished for the purposes of international preliminary examination(under Rules 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

☐ contained in the international application in printed form.

☐ filed together with the international application in computer readable form.

☐ furnished subsequently to this Authority in written form.

☐ furnished subsequently to this Authority in computer readable form.

☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☒ The amendments have resulted in the cancellation of:

☒ the description, pages NONE

☒ the claims, Nos. NONE

☒ the drawings, sheets/~~fig~~ NONE

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

** Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17).*
*** Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.*

WRITTEN [redacted]INION

International [redacted]pplication No.
PCT/US[redacted]10

V. Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. STATEMENT

Novelty (N)	Claims	2-14 and 16-28	YES
	Claims	1 and 15	NO
Inventive Step (IS)	Claims	NONE	YES
	Claims	1-28	NO
Industrial Applicability (IA)	Claims	1-28	YES
	Claims	NONE	NO

2. CITATIONS AND EXPLANATIONS
Please See Continuation Sheet

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

The drawings are objected to under PCT Rule 66.2(a)(iii) as containing the following defects in the form or content thereof: In figure 2, item 44, delete "ECRYPTION" and replace with --ENCRYPTION--. In figure 2, item 64, delete "AYSYMMETRICAL" and replace with --ASYMMETRICAL--.

Claim 15 is objected to under PCT Rule 66.2(a)(iii) as containing the following defect in the form or contents thereof: delete "." in line 1 of page 22 and replace with --;--.

Supplemental Box
(To be used when the space in any of the preceding boxes is not sufficient)

V. 2. Citations and Explanations:

Claims 1 and 15 lack novelty under PCT Article 33(2) as being anticipated by Ganesan, U.S. Patent No. 5,557,678. Ganesan illustrates a cryptographic key split combiner and a process for forming cryptographic keys, comprising: a plurality of key split generators for generating cryptographic key splits (see column 8, lines 30-35 and figure 1, items 33 and 50); a key split randomizer for randomizing the cryptographic keys splits to produce a cryptographic key (see column 8, lines 36-50); wherein each of the key split generators includes means for generating key splits from seed data (see column 8, lines 36-50); and in which at least one of the key split generators is an asymmetric key split generator (see column 8, lines 36-50).

Claims 2, 4, 16, and 18 lack an inventive step under PCT Article 33(3) as being obvious over the prior art as applied in the immediately preceding paragraph and further in view of Hirsch, U.S. Patent No. 5,276,738. As per claims 2 and 16, Ganesan discloses the combiner and process of claims 1 and 15, respectively. However, he does not teach about a random split generator. Hirsch discusses that the plurality of key split generators includes a random split generator for generating a random key split based on reference data (see column 2, lines 35-58). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the combiner and process of Ganesan with the random split generator of Hirsch to provide security of a key with one system with respect to another key of another system (see column 2, lines 58-64). As per claims 4 and 18, Hirsch further describes that the random split generator includes means for generating a pseudorandom sequence based on the reference data (see column 2, lines 23-29). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the combiner and process of Ganesan with the random split generator of Hirsch to generate key values that cannot be easily counterfeited (see column 1, lines 37-40).

Claims 3 and 17 lack an inventive step under PCT Article 33(3) as being obvious over the prior art as applied in the immediately preceding paragraph and further in view of Albert et al., U.S. Patent No. 5,627,894. Ganesan in view of Hirsch describe the combiner and process of claims 2 and 16, respectively. Although Hirsch describes the random key split generator includes means for generating a pseudorandom sequence based on reference data (see column 2, lines 23-29), he does not explicitly mention generating a random sequence. Albert et al. specify generating a random sequence (see column 1, lines 51-67 and column 2, lines 1-2). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the combiner and process of Ganesan in view of Hirsch with the generating of a random sequence of Albert et al. to increase the quality of random numbers with respect to their predictability and their functional link (see column 1, lines 66-67 and column 2, lines 1-2).

Claims 5 and 19 lack an inventive step under PCT Article 33(3) as being obvious over the prior art as applied in the preceding paragraph regarding claims 2, 4, 16, and 18 and further in view of Thomlinson et al., U.S. Patent No. 5,778,069. Ganesan in view of Hirsch describe the combiner and process of claims 2 and 16, respectively. However, neither Ganesan nor Hirsch explicitly show chronological data. Thomlinson et al. disclose generating a key split based on reference data and on chronological data (see column 3, lines 16-23). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the combiner and process of Ganesan in view of Hirsch with the generating of a key split based on chronological data of

Supplemental Box
(To be used when the space in any of the preceding boxes is not sufficient)

Thomlinson et al. to ensure unguessability (see column 3, lines 2-7).

Claims 6, 7, 20 and 21 lack an inventive step under PCT Article 33(3) as being obvious over the prior art as applied in the preceding paragraph regarding claims 2, 4, 16, and 18 and further in view of Ming et al., U.S. Patent No. 5,710,815. As per claims 6 and 20, Ganesan in view of Hirsch describe the combiner and process of claims 2 and 16, respectively. However, neither Ganesan nor Hirsch explicitly delineate static data. Ming et al. discuss generating a key split based on reference data and on static data (see column 4, lines 4-7). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the combiner and process of Ganesan in view of Hirsch with the generating of a key split based on static data of Ming et al. for implementation of viewer access restrictions (see column 7, lines 3-10). As per claims 7 and 21, Ming et al. further disclose a means of updating the static data (see column 4, line 8). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the combiner and process of Ganesan in view of Hirsch with the updating of static data of Ming et al. for synchronizing a first pseudo-random number generator within a transmitting unit and a second pseudo-random number generator within a receiving unit (see column 3, lines 65-67 and column 4, lines 1-4).

Claims 8 and 22 lack an inventive step under PCT Article 33(3) as being obvious over the prior art as applied in the immediately preceding paragraph and further in view of Anshel et al., U.S. Patent No. 5,751,808. Ganesan in view of Hirsch and in view of Ming et al. describe the combiner and process of claims 7 and 21, respectively. Ming et al. describe modifying a divisor of the static data (see column 4, lines 18-20). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the combiner and process of Ganesan in view of Hirsch with the modifying of a divisor of the static data of Ming et al. for synchronizing a first pseudo-random number generator within a transmitting unit and a second pseudo-random number generator within a receiving unit (see column 3, lines 65-67 and column 4, lines 1-4). Anshel et al. show modifying a prime divisor of the static data (see column 11, lines 8-25 and figure 8, item 71). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the combiner and process of Ganesan in view of Hirsch and in view of Ming et al. with modifying a prime number divisor of the static data of Anshel et al. to generate a cryptographically secure sequence at high speed (see column 1, lines 11-12).

Claims 9-12, 14, 23-26, and 28 lack an inventive step under PCT Article 33(3) as being obvious over the prior art as applied in the preceding paragraph regarding claims 1 and 15 and further in view of Vanstone et al., U.S. Patent No. 5,761,305. As per claims 9 and 23, Ganesan discloses the combiner and process of claims 1 and 15, respectively. Although Ganesan describes a means for receiving a prime number (see column 8, lines 37-39), he does not specify a random number. Vanstone et al. elaborates on receiving a prime number and a random number (see column 4, lines 19-29). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the combiner and process of Ganesan with the receiving of a prime number and a random number of Vanstone et al. to avoid an interloper convincing the receiver that he is communicating with the interloper (see column 4, lines 17-18). As per claims 10 and 24, Vanstone et al. further mention a means for performing a polynomial calculation on the prime number and the random number (see column 4, lines 27-28). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the combiner and process of Ganesan with performing a polynomial calculation on the prime number and the random number of Vanstone et al. to avoid an interloper convincing the receiver that he is communicating with the interloper (see column 4, lines 17-18). As per claims 11 and 25, Vanstone also show a means for performing a modulo calculation on the prime number and the random number (see column 4, lines 27-28). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the combiner and process of Ganesan with performing a modulo calculation on the prime number and the random number of Vanstone et al. to avoid an interloper convincing the receiver that he is communicating with the interloper (see column 4, lines 17-18). As per claims 12 and 26, Vanstone et al. moreover embody a means for generating a session key based on the prime number and the random number (see column 4, lines 33-34). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the combiner and process of Ganesan with generating a session key based on the prime number and the random number of Vanstone et al. to avoid an interloper convincing the receiver that he is communicating with the interloper (see column 4, lines 17-18). As per claims 14 and 28, Ganesan then discusses a means for encrypting the random key split with the session key to create an asymmetrical split (see column 5, lines 6-14).

Claims 13 and 27 lack an inventive step under PCT Article 33(3) as being obvious over the prior art as applied in the immediately preceding paragraph and further in view of Hirsch, U.S. Patent No. 5,276,738. As per claims 13 and 27, Ganesan in view of Vanstone et al. discloses the combiner and process of claims 12 and 26, respectively. However, neither Genesan nor Vanstone et al. describe reference data. Hirsch discusses that the plurality of key split generators includes a random split generator for generating a random key split based on reference data (see column 2, lines 35-58). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the combiner and process of Ganesan in view of Vanstone et al. with the random split generator of Hirsch to provide security of a key with one system with respect to another key of another system (see column 2, lines 58-64).

Claims 1-28 meet the criteria set out in PCT Article 33(4) because a cryptographic key split combiner and a process for forming cryptographic keys have use in providing added security against compromising a communications medium by unauthorized entities

Supplemental Box
(To be used when the space in any of the preceding boxes is not sufficient)

(see the description, page 3, lines 26-32).

09/936315

PATENT COOPERATION TREATY

RECEIVED
MAR 22 2001
BY: PCT

From the
INTERNATIONAL PRELIMINARY EXAMINING AUTHORITY

To:
THOMAS M. CHAMPAGNE
RABIN & CHAMPAGNE
1101 14TH STREET, N.W.
SUITE 500
WASHINGTON, DC 20005

INVITATION TO REQUEST RECTIFICATION

(PCT Rule 91.1(d))

	Date of Mailing (*day/month/year*) 20 MAR 2001
Applicant's or agent's file reference STS131PCT	**REPLY DUE** see item 2 and the last paragraph below
International application No. PCT/US00/06110	International filing date (*day/month/year*) 10 March 2000 (10.03.2000)
Applicant TECSEC, INCORPORATED	

1. This International Preliminary Examining Authority has discovered in the international application/in other papers submitted by the applicant/what appears to be an obvious error.

☐ as shown on the attached copy

☒ as specified hereafter:

Please See Continuation Sheet

2. The applicant is hereby **invited to submit a request for rectification** to the following authority:

☐ the receiving Office ☒ this International Preliminary Examining Authority 34 ☐ the International Bureau of WIPO chemin des Colombettes 1211 Geneva 20, Switzerland

HOW TO CORRECT AN ERROR (Rule 26.4(a))

☒ A replacement sheet must be submitted and the rectification must be stated in an accompanying letter drawing attention to the differences between the replaced sheet and the replacement sheet

☐ The rectification may be stated in a letter.

☐ The applicant may choose either of the two possibilities described above.

ATTENTION

No rectification will be made without the express authorization of the competent authority indicated above and (Rule 91.1(g) to (*g-quater*) for further details and for time limits).

Name and mailing address of the IPEA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer Tod R. Swann James R. Matthews Telephone No. (703) 308-0873

Form PCT/IPEA/411 (January 1994)

WRITTEN OPINION

International application No.
PCT/US00/06110

I. Basis of the opinion

1. With regard to the **elements** of the international application:*

☒ the international application as originally filed

☒ the description:
pages 1-19, as originally filed
pages NONE, filed with the demand
pages NONE, filed with the letter of _____.

☒ the claims:
pages 20-23, as originally filed
pages NONE, as amended (together with any statement) under Article 19
pages NONE, filed with the demand
pages NONE, filed with the letter of _____.

☒ the drawings:
pages 1-3, as originally filed
pages NONE, filed with the demand
pages NONE, filed with the letter of _____.

☐ the sequence listing part of the description:
pages NONE, as originally filed
pages NONE, filed with the demand
pages NONE, filed with the letter of _____.

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language _____ which is:

☐ the language of a translation furnished for the purposes of international search (under Rule23.1(b)).

☐ the language of publication of the international application (under Rule 48.3(b)).

☐ the language of the translation furnished for the purposes of international preliminary examination(under Rules 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the written opinion was drawn on the basis of the sequence listing:

☐ contained in the international application in printed form.

☐ filed together with the international application in computer readable form.

☐ furnished subsequently to this Authority in written form.

☐ furnished subsequently to this Authority in computer readable form.

☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☒ The amendments have resulted in the cancellation of:

☒ the description, pages NONE

☒ the claims, Nos. NONE

☒ the drawings, sheets/~~fig~~ NONE

5. ☐ This opinion has been drawn as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).

** Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this opinion as "originally filed."*

WRITTEN OPINION

International application No.
PCT/00/06110

V. Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. STATEMENT

Novelty (N)	Claims	2-14 and 16-28	YES
	Claims	1 and 15	NO
Inventive Step (IS)	Claims	NONE	YES
	Claims	1-28	NO
Industrial Applicability (IA)	Claims	1-28	YES
	Claims	NONE	NO

2. CITATIONS AND EXPLANATIONS
Please See Continuation Sheet

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

The drawings are objected to under PCT Rule 66.2(a)(iii) as containing the following defects in the form or content thereof: In figure 2, item 44, delete "ECRYPTION" and replace with --ENCRYPTION--. In figure 2, item 64, delete "AYSYMMETRICAL" and replace with --ASYMMETRICAL--.

Claim 15 is objected to under PCT Rule 66.2(a)(iii) as containing the following defect in the form or contents thereof: delete "." in line 1 of page 22 and replace with --;--.

Supplemental Box
(To be used when the space in any of the preceding boxes is not sufficient)

TIME LIMIT:
The time limit set for response to a Written Opinion may not be extended. 37 CFR 1.484(d). Any response received after the expiration of the time limit set in the Written Opinion will not be considered in preparing the International Preliminary Examination Report.

V. 2. Citations and Explanations:
Claims 1 and 15 lack novelty under PCT Article 33(2) as being anticipated by Ganesan, U.S. Patent No. 5,557,678. Ganesan illustrates a cryptographic key split combiner and a process for forming cryptographic keys, comprising: a plurality of key split generators for generating cryptographic key splits (see column 8, lines 30-35 and figure 1, items 33 and 50); a key split randomizer for randomizing the cryptographic keys splits to produce a cryptographic key (see column 8, lines 36-50); wherein each of the key split generators includes means for generating key splits from seed data (see column 8, lines 36-50); and in which at least one of the key split generators is an asymmetric key split generator (see column 8, lines 36-50).

Claims 2, 4, 16, and 18 lack an inventive step under PCT Article 33(3) as being obvious over the prior art as applied in the immediately preceding paragraph and further in view of Hirsch, U.S. Patent No. 5,276,738. As per claims 2 and 16, Ganesan discloses the combiner and process of claims 1 and 15, respectively. However, he does not teach about a random split generator. Hirsch discusses that the plurality of key split generators includes a random split generator for generating a random key split based on reference data (see column 2, lines 35-58). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the combiner and process of Ganesan with the random split generator of Hirsch to provide security of a key with one system with respect to another key of another system (see column 2, lines 58-64). As per claims 4 and 18, Hirsch further describes that the random split generator includes means for generating a pseudorandom sequence based on the reference data (see column 2, lines 23-29). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the combiner and process of Ganesan with the random split generator of Hirsch to generate key values that cannot be easily counterfeited (see column 1, lines 37-40).

Claims 3 and 17 lack an inventive step under PCT Article 33(3) as being obvious over the prior art as applied in the immediately preceding paragraph and further in view of Albert et al., U.S. Patent No. 5,627,894. Ganesan in view of Hirsch describe the combiner and process of claims 2 and 16, respectively. Although Hirsch describes the random key split generator includes means for generating a pseudorandom sequence based on reference data (see column 2, lines 23-29), he does not explicitly mention generating a random sequence. Albert et al. specify generating a random sequence (see column 1, lines 51-67 and column 2, lines 1-2). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the combiner and process of Ganesan in view of Hirsch with the generating of a random sequence of Albert et al. to increase the quality of random numbers with respect to their predictability and their functional link (see column 1, lines 66-67 and column 2, lines 1-2).

Claims 5 and 19 lack an inventive step under PCT Article 33(3) as being obvious over the prior art as applied in the preceding paragraph regarding claims 2, 4, 16, and 18 and further in view of Thomlinson et al., U.S. Patent No. 5,778,069. Ganesan in view of Hirsch describe the combiner and process of claims 2 and 16, respectively. However, neither Ganesan nor Hirsch explicitly show

Supplemental Box
(To be used when the space in any of the preceding boxes is not sufficient)

chronological data. Thomlinson et al. disclose generating a key split based on reference data and on chronological data (see column 3, lines 16-23). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was mad to combine the combiner and process of Ganesan in view of Hirsch with the generating of a key split based on chronological data of Thomlinson et al. to ensure unguessability (see column 3, lines 2-7).

Claims 6, 7, 20 and 21 lack an inventive step under PCT Article 33(3) as being obvious over the prior art as applied in the preceding paragraph regarding claims 2, 4, 16, and 18 and further in view of Ming et al., U.S. Patent No. 5,710,815. As per claims 6 and 20, Ganesan in view of Hirsch describe the combiner and process of claims 2 and 16, respectively. However, neither Ganesan nor Hirsch explicitly delineate static data. Ming et al. discuss generating a key split based on reference data and on static data (see column 4, lines 4-7). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the combiner and process of Ganesan in view of Hirsch with the generating of a key split based on static data of Ming et al. for implementation of viewer access restrictions (see column 7, lines 3-10). As per claims 7 and 21, Ming et al. further disclose a means of updating the static data (see column 4, line 8). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the combiner and process of Ganesan in view of Hirsch with the updating of static data of Ming et al. for synchronizing a first pseudo-random number generator within a transmitting unit and a second pseudo-random number generator within a receiving unit (see column 3, lines 65-67 and column 4, lines 1-4).

Claims 8 and 22 lack an inventive step under PCT Article 33(3) as being obvious over the prior art as applied in the immediately preceding paragraph and further in view of Anshel et al., U.S. Patent No. 5,751,808. Ganesan in view of Hirsch and in view of Ming et al. describe the combiner and process of claims 7 and 21, respectively. Ming et al. describe modifying a divisor of the static data (see column 4, lines 18-20). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the combiner and process of Ganesan in view of Hirsch with the modifying of a divisor of the static data of Ming et al. for synchronizing a first pseudo-random number generator within a transmitting unit and a second pseudo-random number generator within a receiving unit (see column 3, lines 65-67 and column 4, lines 1-4). Anshel et al. show modifying a prime divisor of the static data (see column 11, lines 8-25 and figure 8, item 71). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the combiner and process of Ganesan in view of Hirsch and in view of Ming et al. with modifying a prime number divisor of the static data of Anshel et al. to generate a cryptographically secure sequence at high speed (see column 1, lines 11-12).

Claims 9-12, 14, 23-26, and 28 lack an inventive step under PCT Article 33(3) as being obvious over the prior art as applied in the preceding paragraph regarding claims 1 and 15 and further in view of Vanstone et al., U.S. Patent No. 5,761,305. As per claims 9 and 23, Ganesan discloses the combiner and process of claims 1 and 15, respectively. Although Ganesan describes a means for receiving a prime number (see column 8, lines 37-39), he does not specify a random number. Vanstone et al. elaborates on receiving a prime number and a random number (see column 4, lines 19-29). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the combiner and process of Ganesan with the receiving of a prime number and a random number of Vanstone et al. to avoid an interloper convincing the receiver that he is communicating with the interloper (see column 4, lines 17-18). As per claims 10 and 24, Vanstone et al. further mention a means for performing a polynomial calculation on the prime number and the random number (see column 4, lines 27-28). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the combiner and process of Ganesan with performing a polynomial calculation on the prime number and the random number of Vanstone et al. to avoid an interloper convincing the receiver that he is communicating with the interloper (see column 4, lines 17-18). As per claims 11 and 25, Vanstone also show a means for performing a modulo calculation on the prime number and the random number (see column 4, lines 27-28). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the combiner and process of Ganesan with performing a modulo calculation on the prime number and the random number of Vanstone et al. to avoid an interloper convincing the receiver that he is communicating with the interloper (see column 4, lines 17-18). As per claims 12 and 26, Vanstone et al. moreover embody a means for generating a session key based on the prime number and the random number (see column 4, lines 33-34). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the combiner and process of Ganesan with generating a session key based on the prime number and the random number of Vanstone et al. to avoid an interloper convincing the receiver that he is communicating with the interloper (see column 4, lines 17-18). As per claims 14 and 28, Ganesan then discusses a means for encrypting the random key split with the session key to create an asymmetrical split (see column 5, lines 6-14).

Claims 13 and 27 lack an inventive step under PCT Article 33(3) as being obvious over the prior art as applied in the immediately preceding paragraph and further in view of Hirsch, U.S. Patent No. 5,276,738. As per claims 13 and 27, Ganesan in view of Vanstone et al. discloses the combiner and process of claims 12 and 26, respectively. However, neither Genesan nor Vanstone et al. describe reference data. Hirsch discusses that the plurality of key split generators includes a random split generator for generating a random key split based on reference data (see column 2, lines 35-58). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the combiner and process of Ganesan in view of Vanstone et al. with the random split generator of Hirsch to provide security of a key with one system with respect to another key of another system (see column 2, lines 58-64).

Supplemental Box
(To be used when the space in any of the preceding boxes is not sufficient)

Claims 1-28 meet the criteria set out in PCT Article 33(4) because a cryptographic key split combiner and a process for forming cryptographic keys have use in providing added security against compromising a communications medium by unauthorized entities (see the description, page 3, lines 26-32).

PATENT COOPERATION TREATY

09/936315

From the INTERNATIONAL SEARCHING AUTHORITY

To:
THOMAS M. CHAMPAGNE
RABIN & CHAMPAGNE, P.C.
1725 K STREET, N.W.
SUITE 1111
WASHINGTON, DC 20009

AUG 22 2000

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT OR THE DECLARATION

(PCT Rule 44.1)

	Date of Mailing *(day/month/year)* **17 AUG 2000**
Applicant's or agent's file reference STS131PCT	FOR FURTHER ACTION See paragraphs 1 and 4 below
International application No. PCT/US00/06110	International filing date *(day/month/year)* 10 March 2000 (10.03.2000)
Applicant TECSEC, INCORPORATED	

1. ☒ The applicant is hereby notified that the international search report has been established and is transmitted herewith.

Filing of amendments and statement under Article 19:
The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 46):

When? The time limit for filing such amendments is normally 2 months from the date of transmittal of the international search report; however, for more details, see the notes on the accompany sheet.

Where? Directly to the International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland
Facsimile No.: (41-22) 740.14.35

For more detailed instructions, see the notes on the accompanying sheet.

2. ☐ The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect is transmitted herewith.

3. ☐ **With regard to the protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

☐ the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

☐ no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Further action(s):** The applicant is reminded of the following:

Shortly after **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application , or of the priority claim, must reach the International Bureau as provided in rules 90 *bis* 1 and 90 *bis* 3, respectively, before the completion of the technical preparations for international publication.

Within **19 months** from the priority date, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase until 30 months from the priority date (in some Offices even later).

Within **20 months** from the priority date, the applicant must perform the prescribed acts for entry into the national phase before all designated Offices which have not been elected in the demand or in a later election within 19 months from the priority date or could not be elected because they are not bound by Chapter II.

Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer Tod R. Swann *James R. Matthews* Telephone No. (703) 305-9700

Form PCT/ISA/220 (July 1998)

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
THOMAS M. CHAMPAGNE
RABIN & CHAMPAGNE, P.C.
1725 K STREET, N.W.
SUITE 1111
WASHINGTON, DC 20009

PCT

NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT OR THE DECLARATION

(PCT Rule 44.1)

	Date of Mailing *(day/month/year)* 17 AUG 2000
Applicant's or agent's file reference STS131PCT	FOR FURTHER ACTION See paragraphs 1 and 4 below
International application No. PCT/US00/06110	International filing date *(day/month/year)* 10 March 2000 (10.03.2000)
Applicant TECSEC, INCORPORATED	

1. ☒ The applicant is hereby notified that the international search report has been established and is transmitted herewith.

Filing of amendments and statement under Article 19:
The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 46):

When? The time limit for filing such amendments is normally 2 months from the date of transmittal of the international search report; however, for more details, see the notes on the accompany sheet.

Where? Directly to the International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland
Facsimile No.: (41-22) 740.14.35

For more detailed instructions, see the notes on the accompanying sheet.

2. ☐ The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect is transmitted herewith.

3. ☐ **With regard to the protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

☐ the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

☐ no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Further action(s):** The applicant is reminded of the following:

Shortly after **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application , or of the priority claim, must reach the International Bureau as provided in rules 90 *bis* 1 and 90 *bis* 3, respectively, before the completion of the technical preparations for international publication.

Within **19 months** from the priority date, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase until 30 months from the priority date (in some Offices even later).

Within **20 months** from the priority date, the applicant must perform the prescribed acts for entry into the national phase before all designated Offices which have not been elected in the demand or in a later election within 19 months from the priority date or could not be elected because they are not bound by Chapter II.

Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer Tod R. Swann James R. Matthews Telephone No. (703) 305-9700

Form PCT/ISA/220 (July 1998)

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference STS131PCT	**FOR FURTHER ACTION**	see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.
International application No. PCT/US00/06110	International filing date *(day/month/year)* 10 March 2000 (10.03.2000)	(Earliest) Priority Date *(day/month/year)* 11 March 1999 (11.03.1999)
Applicant TECSEC, INCORPORATED		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 5 sheets.

☒ It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the Report**
   a. With regard to the **language**, the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.
   ☐ the international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).
   b. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international search was carried out on the basis of the sequence listing:
   ☐ contained in the international application in written form.
   ☐ filed together with the international application in computer readable form.
   ☐ furnished subsequently to this Authority in written form.
   ☐ furnished subsequently to this Authority in computer readable form.
   ☐ the statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
   ☐ the statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.
2. ☐ **Certain claims were found unsearchable** (See Box I).
3. ☐ **Unity of invention is lacking** (See Box II).
4. With regard to the **title**,
   ☐ the text is approved as submitted by the applicant.
   ☒ the text has been established by this Authority to read as follows:

Please See Continuation Sheet

5. With regard to the **abstract**,
   ☐ the text is approved as submitted by the applicant.
   ☒ the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.

6. The figure of the **drawings** to be published with the abstract is Figure No. 2
   ☒ as suggested by the applicant.
   ☐ None of the figures
   ☐ because the applicant failed to suggest a figure.
   ☐ because this figure better characterizes the invention.

Box III TEXT OF THE ABSTRACT (Continuation of Item 5 of the first sheet)

A cryptographic key split combiner, which includes a number of key split generators (42, 48, and 56) for generating cryptographic key splits (32, 34, 36, 38, and 64) and a key split randomizer for randomizing the cryptographic key splits to produce a cryptographic key (62), and a process for forming cryptographic keys. Each of the key split generators (42, 48 and 56) generates key splits (32, 34, 36, 38, and 64) from seed data (40, 44, 46, 50, 52, 54, 58, and 60). The key split generators may include a random split generator (42) for generating a random key split (32) based on reference data (40) and encryption date/time (44). Other key split generators may include a token split generator (48) for generating a token key split (34) based on label data (46) and organization data (50), a console split generator (56) for generating a console key split (36) based on current maintenance data (52) and previous maintenance data (54), and a biometric split generator for generating a biometric key split (38) based on biometric data (58). All splits may further be based on static data, which may be updated, for example by modifying a prime number divisor of the static data. The label data may be read from a storage medium, and may include user authorization data. The label data may be associated with label categories and sub-categories of addresses, which are meaningful to a user who is specifying or determining the intended recipient(s) of the encrypted information or object. An array associated with a software component object may use key splits (32, 34, 36, 38, and 64) which determine which methods and properties are allowed and control access to the memory address for those allowed methods and properties. The resulting cryptographic key (62) may be, for example, a stream of symbols, at least one symbol block, or a key matrix.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/06110

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) : H04L 9/14, 9/20, 9/30
US CL : 380/30, 47, 268

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 380/30, 44, 46, 47, 264, 268, 286; 708/250, 254, 255, 501, 523

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
SCHNEIER, APPLIED CRYPTOGRAPHY

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Please See Continuation Sheet

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X --- Y	US 5,557,678 A (GANESAN) 17 September 1996 (17.09.1996), column 4, lines 12-67, column 5, lines 1-35, column 8, lines 26-67, column 9, lines 1-23, column 10, lines 40-65, column 11, lines 1-10, figure 2, figure 5.	1, 15 --- 2-14, 16-28
Y	US 5,276,738 A (HIRSCH) 4 January 1994 (04.01.1994), column 1, lines 49-67, column 2, lines 5-7, lines 23-29, 55-58, column 4, lines 38-40, column 8, lines 8-15.	2-8, 13, 16-22, 27
Y	US 5,627,894 A (ALBERT et al.) 6 May 1997 (06.05.1997), column 1, lines 51-67, column 2, lines 1-2, 23-29.	3, 17
Y	US 5,778,069 A (THOMLINSON et al.) 07 July 1998 (07.07.1998), column 3, lines 2-7, 16-23.	5, 19
Y	US 5,710,815 A (MING et al.) 20 Janurary 1998 (20.01.1998), column 3, lines 65-67, column 4, lines 1-8, 18-20, column 7, lines 3-10.	6-8, 20-22
Y	US 5,751,808 A (ANSHEL et al.) 12 May 1998 (12.05.1998), column 1, lines 11-12, column 11, lines 8-25, figure 8, item 71.	8, 22
Y	US 5,761,305 A (VANSTONE et al.) 02 June 1998 (02.06.1998), column 1, lines 10-14, column 3, lines 52-67, column 4, lines 1-4, 60-67, column 5, lines 1-4.	9-14, 23-28
A	US 5,815,573 A (JOHNSON et al.) 29 September 1998 (29.09.1998), column 3, lines 40-67, column 4, lines 1-41, column 6, lines 38-67, column 7, lines 1-33, figure 1.	1-28

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier application or patent published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 July 2000 (11.07.2000)	17 AUG 2000
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer Tod R. Swann James R. Matthews Telephone No. (703) 305-9700

Form PCT/ISA/210 (second sheet) (July 1998)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/06110

C (Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5,857,025 A (ANDERSON et al.) 05 January 1999 (05.01.1999), column 6, lines 30-67, column 7, lines 1-12, figure 1, figure 2.	2-8, 16-22

Continuation of Item 4 of the first sheet: ENCRYPTION METHOD USING AN ASYMMETRIC CRYPTOGRAPHIC KEY SPLIT COMBINER

Continuation of B. FIELDS SEARCHED Item 3: EAST
search terms: asymmetric, private, public, key, split, portion, part, block, component, combine, construct, compose generate

09/936315

PATENT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

14

Applicant's or agent's file reference STS131PCT	FOR FURTHER ACTION	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/US00/06110	International filing date *(day/month/year)* 10 March 2000 (10.03.2000)	Priority date *(day/month/year)* 11 March 1999 (11.03.1999)
International Patent Classification (IPC) or national classification and IPC IPC(7): G 06 F 12/14; G 06 F 17/21; G06 F 17/60 and US Cl.: 713/189; 705/2, 51; 707/500		
Applicant TECSEC, INCORPORATED		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 7 sheets, including this cover sheet.

   ☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of 0 sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of report with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
   - VI ☐ Certain documents cited
   - VII ☒ Certain defects in the international application
   - VIII ☐ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
10 October 2000 (10.10.2000)	16 July 2001 (16.07.2001)
Name and mailing address of the IPEA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703)305-3230	Authorized officer Gail O. Hayes Telephone No. (703) 305-9711

Form PCT/IPEA/409 (cover sheet)(July 1998)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/US00/06110

I. Basis of the report

1. With regard to the **elements** of the international application:*

☒ the international application as originally filed.

☒ the description:
pages 1-19 as originally filed
pages NONE , filed with the demand
pages NONE , filed with the letter of _____.

☒ the claims:
pages 20-23 , as originally filed
pages NONE , as amended (together with any statement) under Article 19
pages NONE , filed with the demand
pages NONE , filed with the letter of _____.

☒ the drawings:
pages 1-3 , as originally filed
pages NONE , filed with the demand
pages NONE , filed with the letter of _____.

☐ the sequence listing part of the description:
pages NONE , as originally filed
pages NONE , filed with the demand
pages NONE , filed with the letter of _____.

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language _____ which is:

☐ the language of a translation furnished for the purposes of international search (under Rule23.1(b)).

☐ the language of publication of the international application (under Rule 48.3(b)).

☐ the language of the translation furnished for the purposes of international preliminary examination(under Rules 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

☐ contained in the international application in printed form.

☐ filed together with the international application in computer readable form.

☐ furnished subsequently to this Authority in written form.

☐ furnished subsequently to this Authority in computer readable form.

☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☒ The amendments have resulted in the cancellation of:

☒ the description, pages NONE

☒ the claims, Nos. NONE

☒ the drawings, sheets/~~fig~~ NONE

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

** Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17).*

*** Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.*

WRITTEN OPINION

International application No.
PCT/US00/06110

V. Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. STATEMENT

Novelty (N)	Claims	2-14 and 16-28	YES
	Claims	1 and 15	NO
Inventive Step (IS)	Claims	NONE	YES
	Claims	1-28	NO
Industrial Applicability (IA)	Claims	1-28	YES
	Claims	NONE	NO

2. CITATIONS AND EXPLANATIONS

Please See Continuation Sheet

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/US00/06110

VII. Certain defects in the international application

The following defects in the form or contents of the international application have been noted:

The drawings are objected to under PCT Rule 66.2(a)(iii) as containing the following defects in the form or content thereof: In figure 2, item 44, delete "ECRYPTION" and replace with --ENCRYPTION--. In figure 2, item 64, delete "AYSYMMETRICAL" and replace with --ASYMMETRICAL--.

Claim 15 is objected to under PCT Rule 66.2(a)(iii) as containing the following defect in the form or contents thereof: delete "." in line 1 of page 22 and replace with --;--.

Supplemental Box
(To be used when the space in any of the preceding boxes is not sufficient)

V. 2. Citations and Explanations:

Claims 1 and 15 lack novelty under PCT Article 33(2) as being anticipated by Ganesan, U.S. Patent No. 5,557,678. Ganesan illustrates a cryptographic key split combiner and a process for forming cryptographic keys, comprising: a plurality of key split generators for generating cryptographic key splits (see column 8, lines 30-35 and figure 1, items 33 and 50); a key split randomizer for randomizing the cryptographic keys splits to produce a cryptographic key (see column 8, lines 36-50); wherein each of the key split generators includes means for generating key splits from seed data (see column 8, lines 36-50); and in which at least one of the key split generators is an asymmetric key split generator (see column 8, lines 36-50).

Claims 2, 4, 16, and 18 lack an inventive step under PCT Article 33(3) as being obvious over the prior art as applied in the immediately preceding paragraph and further in view of Hirsch, U.S. Patent No. 5,276,738. As per claims 2 and 16, Ganesan discloses the combiner and process of claims 1 and 15, respectively. However, he does not teach about a random split generator. Hirsch discusses that the plurality of key split generators includes a random split generator for generating a random key split based on reference data (see column 2, lines 35-58). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the combiner and process of Ganesan with the random split generator of Hirsch to provide security of a key with one system with respect to another key of another system (see column 2, lines 58-64). As per claims 4 and 18, Hirsch further describes that the random split generator includes means for generating a pseudorandom sequence based on the reference data (see column 2, lines 23-29). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the combiner and process of Ganesan with the random split generator of Hirsch to generate key values that cannot be easily counterfeited (see column 1, lines 37-40).

Claims 3 and 17 lack an inventive step under PCT Article 33(3) as being obvious over the prior art as applied in the immediately preceding paragraph and further in view of Albert et al., U.S. Patent No. 5,627,894. Ganesan in view of Hirsch describe the combiner and process of claims 2 and 16, respectively. Although Hirsch describes the random key split generator includes means for generating a pseudorandom sequence based on reference data (see column 2, lines 23-29), he does not explicitly mention generating a random sequence. Albert et al. specify generating a random sequence (see column 1, lines 51-67 and column 2, lines 1-2). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the combiner and process of Ganesan in view of Hirsch with the generating of a random sequence of Albert et al. to increase the quality of random numbers with respect to their predictability and their functional link (see column 1, lines 66-67 and column 2, lines 1-2).

Claims 5 and 19 lack an inventive step under PCT Article 33(3) as being obvious over the prior art as applied in the preceding paragraph regarding claims 2, 4, 16, and 18 and further in view of Thomlinson et al., U.S. Patent No. 5,778,069. Ganesan in view of Hirsch describe the combiner and process of claims 2 and 16, respectively. However, neither Ganesan nor Hirsch explicitly show chronological data. Thomlinson et al. disclose generating a key split based on reference data and on chronological data (see column 3, lines 16-23). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the combiner and process of Ganesan in view of Hirsch with the generating of a key split based on chronological data of

Supplemental Box
(To be used when the space in any of the preceding boxes is not sufficient)

Thomlinson et al. to ensure unguessability (see column 3, lines 2-7).

Claims 6, 7, 20 and 21 lack an inventive step under PCT Article 33(3) as being obvious over the prior art as applied in the preceding paragraph regarding claims 2, 4, 16, and 18 and further in view of Ming et al., U.S. Patent No. 5,710,815. As per claims 6 and 20, Ganesan in view of Hirsch describe the combiner and process of claims 2 and 16, respectively. However, neither Ganesan nor Hirsch explicitly delineate static data. Ming et al. discuss generating a key split based on reference data and on static data (see column 4, lines 4-7). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the combiner and process of Ganesan in view of Hirsch with the generating of a key split based on static data of Ming et al. for implementation of viewer access restrictions (see column 7, lines 3-10). As per claims 7 and 21, Ming et al. further disclose a means of updating the static data (see column 4, line 8). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the combiner and process of Ganesan in view of Hirsch with the updating of static data of Ming et al. for synchronizing a first pseudo-random number generator within a transmitting unit and a second pseudo-random number generator within a receiving unit (see column 3, lines 65-67 and column 4, lines 1-4).

Claims 8 and 22 lack an inventive step under PCT Article 33(3) as being obvious over the prior art as applied in the immediately preceding paragraph and further in view of Anshel et al., U.S. Patent No. 5,751,808. Ganesan in view of Hirsch and in view of Ming et al. describe the combiner and process of claims 7 and 21, respectively. Ming et al. describe modifying a divisor of the static data (see column 4, lines 18-20). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the combiner and process of Ganesan in view of Hirsch with the modifying of a divisor of the static data of Ming et al. for synchronizing a first pseudo-random number generator within a transmitting unit and a second pseudo-random number generator within a receiving unit (see column 3, lines 65-67 and column 4, lines 1-4). Anshel et al. show modifying a prime divisor of the static data (see column 11, lines 8-25 and figure 8, item 71). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the combiner and process of Ganesan in view of Hirsch and in view of Ming et al. with modifying a prime number divisor of the static data of Anshel et al. to generate a cryptographically secure sequence at high speed (see column 1, lines 11-12).

Claims 9-12, 14, 23-26, and 28 lack an inventive step under PCT Article 33(3) as being obvious over the prior art as applied in the preceding paragraph regarding claims 1 and 15 and further in view of Vanstone et al., U.S. Patent No. 5,761,305. As per claims 9 and 23, Ganesan discloses the combiner and process of claims 1 and 15, respectively. Although Ganesan describes a means for receiving a prime number (see column 8, lines 37-39), he does not specify a random number. Vanstone et al. elaborates on receiving a prime number and a random number (see column 4, lines 19-29). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the combiner and process of Ganesan with the receiving of a prime number and a random number of Vanstone et al. to avoid an interloper convincing the receiver that he is communicating with the interloper (see column 4, lines 17-18). As per claims 10 and 24, Vanstone et al. further mention a means for performing a polynomial calculation on the prime number and the random number (see column 4, lines 27-28). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the combiner and process of Ganesan with performing a polynomial calculation on the prime number and the random number of Vanstone et al. to avoid an interloper convincing the receiver that he is communicating with the interloper (see column 4, lines 17-18). As per claims 11 and 25, Vanstone also show a means for performing a modulo calculation on the prime number and the random number (see column 4, lines 27-28). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the combiner and process of Ganesan with performing a modulo calculation on the prime number and the random number of Vanstone et al. to avoid an interloper convincing the receiver that he is communicating with the interloper (see column 4, lines 17-18). As per claims 12 and 26, Vanstone et al. moreover embody a means for generating a session key based on the prime number and the random number (see column 4, lines 33-34). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the combiner and process of Ganesan with generating a session key based on the prime number and the random number of Vanstone et al. to avoid an interloper convincing the receiver that he is communicating with the interloper (see column 4, lines 17-18). As per claims 14 and 28, Ganesan then discusses a means for encrypting the random key split with the session key to create an asymmetrical split (see column 5, lines 6-14).

Claims 13 and 27 lack an inventive step under PCT Article 33(3) as being obvious over the prior art as applied in the immediately preceding paragraph and further in view of Hirsch, U.S. Patent No. 5,276,738. As per claims 13 and 27, Ganesan in view of Vanstone et al. discloses the combiner and process of claims 12 and 26, respectively. However, neither Genesan nor Vanstone et al. describe reference data. Hirsch discusses that the plurality of key split generators includes a random split generator for generating a random key split based on reference data (see column 2, lines 35-58). Therefore, it would have been obvious to one of ordinary skill in the computer art at the time the invention was made to combine the combiner and process of Ganesan in view of Vanstone et al. with the random split generator of Hirsch to provide security of a key with one system with respect to another key of another system (see column 2, lines 58-64).

Claims 1-28 meet the criteria set out in PCT Article 33(4) because a cryptographic key split combiner and a process for forming cryptographic keys have use in providing added security against compromising a communications medium by unauthorized entities

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/US00/06110

Supplemental Box
(To be used when the space in any of the preceding boxes is not sufficient)

(see the description, page 3, lines 26-32).

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		